

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A network system providing integration, comprising:
 - a client computer;
 - a server;
 - a server-side cryptographic function providing cryptographic services located on the server;
 - a PKI-Bridge providing an interface between the server and the server-side cryptographic function;
 - a remote access switch providing an interface between the client computer and the server;
 - a client-side cryptographic function providing cryptographic services located on the client computer;
 - a dial-up client providing dialing services to access the remote access switch; and
 - a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function, wherein
the server-side cryptographic function generates a challenge string,
the client-side cryptographic function generates a signed response string in response to the challenge string,
the custom script dynamically linked library encodes and divides the signed response string to obtain a plurality of packets,
the PKI-Bridge combines and decodes the plurality of packets to obtain a reconstructed signed response string, and
the server-side cryptographic function verifies the reconstructed signed response string.
2. (Previously Amended) The network system of claim 1, further comprising:
 - a security device holding authentication information; and
 - a security device reader attached to the client computer for reading the security device.

3. (Original) The network system of claim 2, wherein a certificate is stored on the security device.
4. (Original) The network system of claim 2, wherein the security device is a smart card.
5. (Original) The network system of claim 1, further comprising:
a directory service accessed by the server-side cryptographic function.
6. (Original) The network system of claim 5, wherein the directory service is lightweight directory access protocol compliant.
7. (Original) The network system of claim 1, wherein the client-side cryptographic function and the server-side cryptographic function employ the same cryptographic scheme.
8. (Currently Amended) The network system of claim 1, wherein the server-side cryptographic function uses a random number generator to generate [[a]] the challenge string.
9. (Currently Amended) The network system of claim 1, wherein a client-side cryptographic function uses a random number generator to generate [[a]] the signed response string.
10. (Cancelled)
11. (Cancelled)
12. (Cancelled)
13. (Original) The network system of claim 1, wherein the dial-up client operates in terminal mode.
14. (Currently Amended) A network system providing integration, comprising:
a client computer;
a server;
a server-side cryptographic function providing cryptographic services located on the
server;

a PKI-Bridge providing an interface between the server and the server-side cryptographic function;

a remote access switch providing an interface between the client computer and the server;

a client-side cryptographic function providing cryptographic services located on the client computer;

a dial-up client providing dialing services to access the remote access switch;

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function;

a security device holding authentication information;

a security device reader attached to the client computer for reading the security device;

and

a directory service accessed by the server-side cryptographic function, wherein
the server-side cryptographic function generates a challenge string,
the client-side cryptographic function generates a signed response string in
response to the challenge string,
the custom script dynamically linked library encodes and divides the signed
response string to obtain a plurality of packets,
the PKI-Bridge combines and decodes the plurality of packets to obtain a
reconstructed signed response string, and
the server-side cryptographic function verifies the reconstructed signed response
string.

15. (Currently Amended) A client computer comprising:

a dial-up client providing dialing services to the client computer;

a client-side cryptographic function providing cryptographic services located on the client computer; and

a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function, wherein
the client-side cryptographic function generates a signed response string, and
the custom script dynamically linked library encodes and divides the signed
response string to obtain a plurality of packets.

16. (Previously Amended) The client computer of claim 15, further comprising:
a security device reader attached to the client computer for reading a security device.
17. (Currently Amended) The client computer of claim ~~[[15]]~~ 16, wherein ~~[[a]]~~ the security device is a smart card.
18. (Previously Amended) The client computer of claim 15, wherein the custom script dynamically linked library comprises a SDLogin component and a SDSetupDial component.
19. (Original) The client computer of claim 15, wherein the dial-up client automates the authentication process using a hidden terminal operating in terminal mode.
20. (Currently Amended) A client computer comprising:
a dial-up client providing dialing services to the client computer;
a client-side cryptographic function providing cryptographic services located on the client computer;
a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function; and
a security device reader attached to the client computer for reading a security device,
wherein
the client-side cryptographic function generates a signed response string, and
the custom script dynamically linked library encodes and divides the signed response string to obtain a plurality of packets.
21. (Currently Amended) A server comprising:
a server-side cryptographic function providing cryptographic services located on the server; and
a PKI-Bridge providing an interface between the server and the server-side cryptographic function, wherein
the server-side cryptographic function generates a challenge string,
the PKI-Bridge combines and decodes a plurality of packets to obtain a reconstructed signed response string which is a response to the challenge string, and

the server-side cryptographic function verifies the reconstructed signed response string.

22. (Original) The server of claim 21, further comprising:
a directory service accessed by the server-side cryptographic function.
23. (Currently Amended) A server comprising:
a server-side cryptographic function providing cryptographic services located on the server;
a PKI-Bridge providing an interface between the server and the server-side cryptographic function; and
a directory service accessed by the server-side cryptographic function, wherein the server-side cryptographic function generates a challenge string, the PKI-Bridge combines and decodes a plurality of packets to obtain a reconstructed signed response string which is a response to the challenge string, and the server-side cryptographic function verifies the reconstructed signed response string.
24. (Currently Amended) A method of integrating via a dial-up interface, comprising:
sending session initiation information from a dial-up client to a PKI-Bridge;
checking session initiation information by the PKI-Bridge;
generating a challenge string by a server-side cryptographic function;
forwarding the challenge string to a custom script dynamically linked library;
forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;
utilizing a private key from a security device;
generating a response string in response to the challenge string;
signing the response string with the private key of a dial-in user to obtain a signed response string;
forwarding [[a]] the signed response string to the custom script dynamically linked library;
encoding the signed response string to obtain an encoded signed response string;

dividing the encoded signed response string into a plurality of packets;
forwarding the plurality of packets to the PKI-Bridge;
combining the plurality of packets to obtain a reconstructed encoded signed response string;
decoding the reconstructed encoded signed response string to obtain a reconstructed signed response string;
~~reconstructing the signed response string from packets;~~
forwarding ~~[[a]]~~ the reconstructed signed response string to the server-side cryptographic function;
obtaining a public key of the dial-in user; and
verifying the reconstructed signed response string based on the public key using the server-side cryptographic function.

25. (Previously Amended) The method of claim 24, further comprising:
reading the security device by a security device reader.
26. (Cancelled)
27. (Cancelled)
28. (Original) The method of claim 24, further comprising:
forwarding the challenge string to the dial-up client; and
forwarding the challenge string to the PKI-Bridge.
29. (Currently Amended) The method of claim 24, further comprising:
forwarding the plurality of packets from the custom script dynamically linked library.
30. (Original) The method of claim 24, wherein the security device is a smart card.
31. (Original) The method of claim 24, wherein the session initiation information comprises version information and a distinguished name.
32. (Original) The method of claim 24, wherein the public key is stored on a directory service.

33. (Original) The method of claim 32, wherein the directory service is lightweight directory access protocol compliant.
34. (Currently Amended) A method of integrating via a dial-up interface, comprising:
sending session initiation information from a dial-up client to a PKI-Bridge;
checking session initiation information by the PKI-Bridge;
generating a challenge string by a server-side cryptographic function;
forwarding the challenge string to a custom script dynamically linked library;
forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;
utilizing a private key from a security device;
generating a response string in response to the challenge string;
signing the response string with the private key of a dial-in user to obtain a signed response string;
forwarding [[a]] the signed response string to the custom script dynamically linked library;
encoding the signed response string to obtain an encoded signed response string;
dividing the encoded signed response string into a plurality of packets;
forwarding the plurality of packets to the PKI-Bridge;
combining the plurality of packets to obtain a reconstructed encoded signed response string;
decoding the reconstructed encoded signed response string to obtain a reconstructed signed response string;
~~reconstructing the signed response string from packets~~;
forwarding [[a]] the reconstructed signed response string to the server-side cryptographic function;
obtaining a public key of the dial-in user; and
verifying the reconstructed signed response string based on the public key using the server-side cryptographic function.
reading the security device by a security card reader;
~~encoding the signed response string~~;
~~decoding the signed response string~~;

forwarding the challenge string to the dial-up client;
forwarding the challenge string to the PKI-Bridge; and
forwarding the plurality of packets from the custom script dynamically linked library.

35. (Currently Amended) An apparatus of integrating via a dial-up interface, comprising:
- means for sending session initiation information from a dial-up client to a PKI-Bridge;
 - means for checking session initiation information by the PKI-Bridge;
 - means for generating a challenge string by a server-side cryptographic function;
 - means for forwarding the challenge string to a custom script dynamically linked library;
 - means for forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library;
 - means for utilizing a private key from a security device;
 - means for generating a response string in response to the challenge string;
 - means for signing the response string with the private key of a dial-in user to obtain a signed response string;
 - means for forwarding [[a]] the signed response string to the custom script dynamically linked library;
 - means for encoding the signed response string to obtain an encoded signed response string;
 - means for dividing the encoded signed response string into a plurality of packets;
 - means for forwarding the plurality of packets to the PKI-Bridge;
 - means for combining the plurality of packets to obtain a reconstructed encoded signed response string;
 - means for decoding the reconstructed encoded signed response string to obtain a reconstructed signed response string;
 - ~~means for reconstructing the signed response string from packets;~~
 - means for forwarding [[a]] the reconstructed signed response string to the server-side cryptographic function;
 - means for obtaining a public key of the dial-in user; and
 - means for verifying the reconstructed signed response string based on the public key using the server-side cryptographic function.